Where We Are:
Big Data and Online Privacy

THE EVOLUTION OF STORED DATA
PROTECTING YOURSELF ONLINE
The Computer Memory Cost Implosion

Historical Cost of Computer Memory and Storage

Year

Memory Price ($/MB)

- Flip-Flops
- Core
- ICs on boards
- SIMMs
- DIMMs
- Big Drives
- Floppy Drives
- Small Drives
- Flash Memory
The Evolution of Stored Data

<table>
<thead>
<tr>
<th>local</th>
<th>networked / distributed</th>
</tr>
</thead>
<tbody>
<tr>
<td>use-specific</td>
<td>detailed / overall</td>
</tr>
<tr>
<td>short-term</td>
<td>(very) long-term</td>
</tr>
<tr>
<td>user-accessible</td>
<td>anyone-accessible</td>
</tr>
<tr>
<td>bulky</td>
<td>(very) portable</td>
</tr>
<tr>
<td>one copy</td>
<td>(very) many copies</td>
</tr>
<tr>
<td>hard to copy</td>
<td>(very) easy to copy</td>
</tr>
<tr>
<td>authority-verified</td>
<td>anyone-verified</td>
</tr>
</tbody>
</table>
# Stored Data: Joys and Perils

<table>
<thead>
<tr>
<th>Joys</th>
<th>Characteristics</th>
<th>Perils</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store anything easily</td>
<td>Storage easy</td>
<td>Store false / misleading easily</td>
</tr>
<tr>
<td>Find anything easily</td>
<td>Storage easy</td>
<td>Find false / misleading easily</td>
</tr>
<tr>
<td>Spread anything easily</td>
<td>Store anything</td>
<td>Integrate / reconstruct easy</td>
</tr>
<tr>
<td>Everything remembered</td>
<td>Store anytime</td>
<td>Steal anything easily</td>
</tr>
<tr>
<td>Personal customization</td>
<td>Store forever</td>
<td>Spread impossible to stop</td>
</tr>
</tbody>
</table>

- Appropriate governance and laws are critical in mitigating the perils above; so is responsible behaviour by people.
Cryptography: A Privacy Survival Tool

- Protect personal data and identity using cryptography.
- Symmetric (one key) cryptography:

Pros:
- Computationally quick
- Provably uncrackable in certain situations

Cons:
- Key can be stolen / deduced
- Available software may be compromised by national security agencies
Cryptography: A Privacy Survival Tool (Cont’d)

- Asymmetric (two key) cryptography:

![Diagram of asymmetric cryptography]

**Pros:**
- Provides secure messages and signatures
- Not impossible but very hard to crack
- Much software available

**Cons:**
- Computationally more expensive
- Keys can be stolen / deduced
- Available software is often illegal
Cryptography: A Privacy Survival Tool (Cont’d)

- Secure messages (encrypt message with B’s public key):

  - messageA → Encrypt → ciphertext → Decrypt → messageA
    - A → keyB (public) → B

- Secure signature (encrypt signature with A’s private key):

  - signatureA → Encrypt → ciphertext → Decrypt → signatureA
    - A → keyA (private) → B
Surviving and Thriving with Big Data

- Learn crap detection and online research skills (Rheingold)
- Limit degree of personal (esp. commercial) exposure online
  - Know privacy settings and use appropriately
- Limit types of personal exposure online
- Use encryption where possible (and legal)
- Update your computing devices with security fixes regularly
- Be aware of what’s going on privacy-wise both technologically and commercially

“Don’t Panic” – *The Hitchiker’s Guide to the Galaxy*
“Let’s be careful out there” – *Hill Street Blues*